TITLE OF THE INVENTION

ENCRYPTION METHOD, DECRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATION SYSTEM AND ENCRYPTION DEVICE

BACKGROUND OF THE INVENTION

The present invention relates to an encryption method for encrypting a plaintext into a ciphertext, a decryption method for decrypting a ciphertext into a plaintext, a cryptographic communication system using these encryption method and decryption method, an encryption device for performing the encryption method, and a memory product/data signal embodied in carrier wave for recording/transferring an operation program of the encryption method.

In the modern society, called a highly information - oriented society, based on a computer network, important business documents and image information are transmitted and communicated in a form of electronic information. Such electronic information can be easily copied, so that it tends to be difficult to discriminate its copy and original from each other, thus bringing about an important issue of data integrity. In particular, it is indispensable for establishment of a highly information oriented society to implement such a computer network that meets the factors of "sharing of computer resources," "multi-accessing," and "globalization," which however includes various factors contradicting the problem of data integrity among the parties concerned. In an attempt to eliminate those contradictions, encrypting technologies which have been mainly used in the past military

and diplomatic fields in the human history are attracting world attention as an effective method for that purpose.

A cipher communication is defined as exchanging information in such a manner that no one other than the parties concerned can understand the meaning of the information. In the field of cipher communication, encryption is defined as converting an original text (plaintext) that can be understood by anyone into a text (ciphertext) that cannot be understood by the third party and decryption is defined as restoring a ciphertext into a plaintext, and cryptosystem is defined as the overall processes covering both encryption and decryption. The encrypting and decrypting processes use secret information called an encryption key and a decryption key, respectively. Since the secret decryption key is necessary in decryption, only those knowing this decryption key can decrypt ciphertexts, thus maintaining data security.

The encryption scheme is roughly classified into two types: common-key cryptosystem and public-key cryptosystem. In a common-key cryptosystem, an encryption key and a decryption key are identical with each other, and a sender and a recipient perform cryptographic communications by possessing an identical common key. The sender encrypts a plaintext based on a secret common key and transmits the resultant ciphertext to the recipient, and then the recipient decrypts the ciphertext into the original plaintext by using this common key.

On the other hand, in a public-key cryptosystem, an encryption key and a decryption key are different from each other, and cryptographic communications are performed by encrypting a plaintext by the sender

with the use of a publicized public key of the recipient and decrypting the resultant ciphertext by the recipient with the use of its own secret key. The public key is a key used for encryption and the secret key is a key used for decrypting the ciphertext transformed by the public key, and the ciphertext transformed by the public key can be decrypted only by the secret key.

Regarding the product-sum type cryptosystem using an operation on an integer ring, which is one of the public-key cryptosystems, new schemes and attacking methods have been proposed one after another. In particular, development of encryption/decryption techniques capable of performing high-speed decryption has been desired so as to process a large quantity of information in a short time. Then, the present inventors proposed an encryption method and a decryption method of the product-sum type cryptosystem, which enable high-speed decryption processing by using multi-adic numbers (Japanese Patent Application Laid-Open No. 2000-89668).

The process of the encryption method and the decryption method is performed as follows. A plaintext to be encrypted is divided into K parts, thereby obtaining a plaintext vector $m = (m_1, m_2, ..., m_K)$. Using a base product generated by bases b_i $(1 \leqq i \leqq K)$ and using random numbers v_i, the $B_i = v_i\, b_1\, b_2 \ldots b_i$ are defined. Using a prime number P, a random number w, and the B_i, public keys c_i are calculated by $c_i \equiv w\, B_i \pmod P$. Here, the c_i are public keys while the b_i, v_i, P, and w are secret keys. Using the public keys c_i, a sender encrypts to obtain a ciphertext $C = m_1 c_1 + m_2 c_2 + \ldots + m_K c_K$. A recipient calculates an intermediate decrypted text $M \equiv w^{-1} C \pmod$

P), thereby to decrypt by a sequential decryption algorithm. As such, the plaintext is expressed by multi-adic numbers, whereby a high-speed decryption can be performed.

Further, in order to prepare against low-density attacks using the LLL (Lenstra-Lenstra-Lovasz) algorithm, the present inventors have proposed an improvement of the above-mentioned encryption method (Japanese Patent Application No.11-173338(1999), referred to as "prior example" hereafter). This prior example is a reduced product-sum type cryptoscheme using error correcting codes, and includes the following alteration to the above-mentioned encryption method and decryption method.

1. Each divided plaintext to be encrypted is error-correction encoded, and used as the above-mentioned m_i.

2. An appropriate number of reduced bases are used for the bases $\{b_i\}$ after a predetermined position, and normal bases are used otherwise. Here, the reduced bases and the normal bases satisfy $m_{i-1} \geqq b_i$ and $m_{i-1} < b_i$, respectively.

3. The m_i indecryptable due to the influence of the reduced bases are decrypted using the capability of the error correcting codes.

In the prior example, it has been found that the m_i can be decrypted up to the position of the firstly appearing reduced base. Thus, despite that the firstly appearing reduced base is preferred to locate at a most possible ascending position, such an approach requires a large capability of error correction, thereby causing a problem of impracticality.

However, such a technique using reduced bases permits the density

(input plaintext length / ciphertext length) to be increased by increasing the redundancy of the plaintext, and hence is an effective technique expected to be capable of increasing the resistance to attacks depending on the LLL algorithm. Thus, the present inventors have been researching further techniques of the reduced product-sum type cryptoscheme.

BRIEF SUMMARY OF THE INVENTION

An object of the present invention is to provide: an encryption method and a decryption method capable of avoiding the problem in the prior example, having resistance to attacks depending on the LLL algorithm, and performing high-speed encryption and decryption; a cryptographic communication system and an encryption device using the same; and a memory product/data signal embodied in carrier wave for recording/transferring an operation program of the encryption method.

The prior example of the reduced product-sum type cryptoscheme using error correcting codes has a higher density than a conventional product-sum type cryptoscheme. Accordingly, it had been thought to be resistant to attacks depending on the LLL algorithm, but has been found to be decryptable. The decryptability results from that the reduced bases are located in the last part continuously. Thus, it is concluded that the reduced bases are to be located in a rather forward part in order to effectively increase the resistance to attacks depending on the LLL algorithm. However, in the prior example, the locating of reduced bases in a forward part requires a larger capability of error correction.

The proposal in the present invention is a reduced product-sum

type cryptoscheme using an extended transformation of a plaintext. The present invention introduces a new technique of the extended transformation in place of the error correction coding. A predetermined transformation is applied on a plaintext vector to be encrypted, thereby generating a transformation vector for increasing the density, thereby performing an extended transformation. Then, a ciphertext is generated by the product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector. In the decryption of the ciphertext, reduced parts, to which an ordinary decryption method is inapplicable, are reproduced according to the above-mentioned predetermined transformation.

In the present invention, the technique of extended transformation of plaintext permits arranging of more reduced bases. Thus, with keeping the high speed in encryption and decryption, the density can be easily set to high to increase the resistance to attacks depending on the LLL algorithm. Further, a complicated encryption/decryption process like error correction coding is unnecessary, and hence encryption/decryption can be carried out easily.

The above and further objects and features of the present invention will more fully be apparent from the following detailed description with accompanying drawings.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. 1 is a schematic diagram showing a situation of

communication between two entities in accordance with the present invention.

FIG. 2 is a diagram showing the configuration of an embodiment of a memory product of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The embodiments of the present invention are described below in detail.

FIG. 1 is a schematic diagram showing a situation that an encryption method adopting the reduced product-sum type cryptoscheme in accordance with the present invention is used in the information communication between entities a, b. In the example of FIG. 1, one entity a encrypts a plaintext X into a ciphertext C, and sends the ciphertext C through a communication channel 1 to another entity b. The entity b then decrypts the ciphertext C into the original plaintext X.

The entity a on the sender side comprises: a plaintext divider 2 for dividing a plaintext X into a plurality of divided plaintexts thereby to obtain a plurality of messages $m_1, m_3, ..., m_{2j-1}, ...$; a dummy message generator 3 for generating dummy messages $m_2, m_4, ..., m_{2j}, ...$ from those odd-number-th messages $m_1, m_3, ..., m_{2j-1}, ...$ in order to increase the density; and an encryptor 4 for generating a ciphertext C using these messages $m_1, m_2, m_3, m_4, ..., m_{2j-1}, m_{2j}, ..., m_K$ and public keys $c_1, c_2, ..., c_K$. On the other hand, the entity b on the recipient side comprises a decryptor 5 for calculating the messages m_i $(1 \leqq i \leqq K)$ according to a branching sequential decryption algorithm described later thereby to decrypt the sent

ciphertext C into the original plaintext X.

The detail of the technique is described below.

[Preparation]

Secret keys and public keys are prepared as follows.

- Secret keys: $\{b_i\}$, $\{v_j\}$, P, w
- Public keys: $\{c_j\}$, $f(\cdot)$

Let the size of each message m_i be e bits, then each message m_i satisfies the following (1).

$$m_i < 2^e \qquad \cdots(1)$$

First, the plaintext X is divided, thereby obtaining the odd-number-th messages $m_1, m_3, \ldots, m_{2j-1}, \ldots$. Next, using the message generating function $f(\cdot)$, the even-number-th messages $m_2, m_4, \ldots, m_{2j}, \ldots$ are generated from the odd-number-th messages $m_1, m_3, \ldots, m_{2j-1}, \ldots$, thereby carrying out the extended transformation of the plaintext. Here, the even-number-th messages $m_2, m_4, \ldots, m_{2j}, \ldots$ are dummy messages for increasing the density. The number of truly effective messages is expressed by the following (2) with the total number K of the messages.

$$\left\lfloor \frac{K+1}{2} \right\rfloor \quad \cdots (2)$$

Further, the bases b_i are assumed to be integers satisfying the following (3).

$$b_i = \begin{cases} 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \\ \qquad\qquad (i = 2j) \\ 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'},\ e' < e) \\ \qquad\qquad (i = 2j-1) \end{cases} \quad \cdots (3)$$

Multiplying a base product $b_1 b_2 \ldots b_i$ by a random number v_i, a base vector $B = (B_1, B_2, \ldots, B_K)$ is defined by the following (4).

$$B_i = v_i b_1 b_2 \ldots b_i \quad \cdots(4)$$

Here, the random numbers v_i are set so that the components B_i shown in the above-mentioned (4) are in the same order of magnitude with each other, while $\gcd(v_i, b_{i+1})=1$ is requested.

Using the random number w, the public keys c_i are obtained by the modulo transformation shown in the following (5).

$$c_i \equiv w B_i \pmod{P} \cdots(5)$$

[Encryption]

A ciphertext C is obtained by a product-sum operation using the messages m_i and public keys c_i. Specifically, the ciphertext C is expressed by the following (6).

$$C = m_1 c_1 + m_2 c_2 + \ldots + m_K c_K \quad \cdots(6)$$

[Decryption]

Decryption processing is carried out as follows. An intermediate decrypted text M for the ciphertext C is calculated by the following (7).

$$M \equiv w^{-1} C \pmod{P} \quad \cdots(7)$$

Then, the decryption into the messages m_i is performed according to a branching sequential decryption algorithm shown in the following (8).

[Branching Sequential Decryption Algorithm]

Step 1

$$M_1 = \frac{M}{b_1}$$

$$m_1 \equiv M_1 v_1^{-1} \pmod{b_2}$$

Step i ($2 \leqq i \leqq K-1$)

$$M_i = \frac{M_{i-1} - m_{i-1} v_{i-1}}{b_i}$$

$$m_i = \begin{cases} M_i v_i^{-1} \pmod{b_{i+1}} & (i = 2j-1) \\ f(m_{i-1}) & (i = 2j) \end{cases} \quad (8)$$

Step K

K : even number

no processing

K : odd number

$$M_K = \frac{M_{K-1} - m_{K-1} v_{K-1}}{b_K}$$

$$m_K = M_K v_K^{-1}$$

In this algorithm, the odd-number-th messages m_i are decrypted by a conventional technique, and the even-number-th messages m_i are decrypted by $m_i = f(m_{i-1})$ using the message generating function $f(\cdot)$.

The message generating function $f(\cdot)$ is discussed below. In order for an encryption method of the present invention to have a high resistance to attacks depending on the LLL algorithm, the $f(\cdot)$ shall not be linear. For example, in case of the identity transformation $f(\cdot)$, that is, in case that $m_{2j} = m_{2j-1}$, the ciphertext C can be rewritten as the following (9). Accordingly, by changing the number of the public keys into the number shown in the following (11) by the substitution shown in the following (10), and by applying a low-density attack, the plaintext can be obtained.

$$C = m_1 c_1 + m_2 c_2 + \cdots\cdots + m_K c_K = m_1 (c_1 + c_2) + \cdots\cdots + m_{K-1} (c_{K-1} + c_K) \cdots (9)$$

$$c_i' = c_{2i-1} + c_{2i} \left(i \leqq \left\lfloor \frac{K+1}{2} \right\rfloor \right) \cdots (10)$$

$$\left\lfloor \frac{K+1}{2} \right\rfloor \cdots (11)$$

However, a non-linearity of the $f(\cdot)$ is not necessarily sufficient for security. For example, in case that $f(x) = a x + b$ (for example, when the $f(\cdot)$ inverts each bit of the messages m_i, $a = -1$ and $b = 2^e - 1$), the ciphertext C can be rewritten as the following (12), and the following (13) and (14) are obtained. Accordingly, by changing the number of the public keys into the number shown in the following (15), and by applying a similar low-density attack, the plaintext can be obtained.

$$C = m_1 (c_1 + a c_2) + \cdots\cdots + b (c_2 + c_4 + \cdots + c_K) \quad \cdots (12)$$

$$C' = C - b \sum_{j=1}^{\lfloor (K+1)/2 \rfloor} c_{2j} \quad \cdots (13)$$

$$c_t' = c_{2t+1} + a c_{2t+2} \quad \cdots (14)$$

$$\left\lfloor \frac{K+1}{2} \right\rfloor \quad \cdots (15)$$

Examples of a safe message generating function f(·) are shown in the following (16) and (17). Here, the q is a prime number of e bits, and the u is an integer of e bits.

$$f(x) = x^2 \bmod q \quad \cdots (16)$$

$$f(x) = x \oplus u \quad \cdots (17)$$

(⊕ : exclusive OR operation of each bit)

The message generating function f(·) may be made public by a reliable center or an entity. Since the bit operation in the f(·) is a non-linear transformation on an integer ring, when a logical operation such as shown in the above-mentioned (17) is introduced, the entity may make public the u alone corresponding to the f(·) with a parameter u which is made public by the center.

Next, the encryption rate and the density in an encryption method of the present invention is discussed below. Encryption rate r in a reduced product-sum type cryptography is defined by original plaintext length / ciphertext length. Density ρ is defined by plaintext length input into reduced product-sum type cryptography / ciphertext length. In the scheme

of the present invention, the density ρ is defined by extended plaintext length / ciphertext length. Here, plaintext length L_P, extended plaintext length L_E, and ciphertext length L_C are defined by the following (18), (19), and (20), respectively. Then, encryption rate r and density ρ are expressed by the following (21) and (22), respectively.

$$L_P = \left\lfloor \frac{K+1}{2} \right\rfloor e \quad \cdots (18)$$

$$L_E = K e \quad \cdots (19)$$

$$L_C \geqq \begin{cases} e + \log_2 K + \dfrac{Ke}{2} + \dfrac{(K-2)e'}{2} & (K: \text{even number}) \\ e + \log_2 K + \dfrac{(K-1)e}{2} + \dfrac{(K-1)e'}{2} & (K: \text{odd number}) \end{cases} \quad \cdots (20)$$

$$r \leqq \frac{L_P}{L_C} \fallingdotseq \frac{e}{e + e' + (\log_2 K)/K} \quad \cdots (21)$$

$$\rho = \frac{L_E}{L_C} \quad \cdots (22)$$

In the cryptoscheme of the present invention, when the value e'/e and hence the bit size e' of the reduced bases becomes small, the encryption rate r increases as well as the density ρ. Accordingly, the contraction of reduced base size permits a high resistance to attacks depending on the

LLL algorithm.

In an encryption method of the present invention, from the above-mentioned (20) and (22), the density ρ exceeds 1 even in the case of the minimum block number K=3. Thus, a high resistance is expected to attacks depending on the LLL algorithm. In this case, if e=64 and e'/e= α, the ciphertext length Lc satisfies the following condition (23). This provides a design of an epoch-making cryptoscheme having a far smaller block size than that of prior art public-key cryptography.

$$L_C = 128 + 1.6 + 64\alpha < 194 \quad \cdots(23)$$

FIG. 2 is a diagram showing the configuration of an embodiment of a memory product in accordance with the present invention. The program illustrated here contains in the above mentioned example the processes of dividing the plaintext to be encrypted thereby to obtain the odd-number-th messages; generating the even-number-th messages from the odd-number-th messages using the message generating function f(·); and generating the product-sum type ciphertext using these messages and the public keys; or contains the process of decrypting the ciphertext into the original plaintext according to the above-mentioned branching sequential decryption algorithm, and further recorded in a memory product described below. A computer 20 is provided in an entity on the sender side or the recipient side.

In FIG. 2, a memory product 21 is composed of, for example, a server computer on the WWW (World Wide Web) installed apart from the installed location of the computer 20. In the memory product 21, a program 21a described above is recorded. The program 21a read out from the

memory product 21 via a transfer medium 24 such as a communication line controls the computer 20 so as to generate a ciphertext from a plaintext or decrypt a ciphertext into a plaintext.

A memory product 22 provided in the interior of the computer 20 is composed of a disk drive, a ROM, or the like built in. In the memory product 22, a program 22a described above is recorded. The program 22a read out from the memory product 22 controls the computer 20 so as to generate a ciphertext from a plaintext or decrypt a ciphertext into a plaintext.

A memory product 23 used in the loaded state into a disk drive 20a provided in the computer 20 is composed of an magneto-optical disk, a CD-ROM, a flexible disk, or the like portable. In the memory product 23, a program 23a described above is recorded. The program 23a read out from the memory product 23 controls the computer 20 so as to generate a ciphertext from a plaintext or decrypt a ciphertext into a plaintext.

Although the description of the above-mentioned example has been made for a case of cryptographic communication system, an encryption method of the present invention is obviously applicable also in a case that a plaintext is encrypted into a ciphertext and that the generated ciphertext is merely recorded.

As described above, in the present invention, encryption is performed by making use of the extended transformation of plaintext, which increases the resistance to attacks depending on the LLL algorithm in comparison with the prior example. Further, in contrast to the prior example using error correction coding, a complicated encryption/decryption process is unnecessary. Thus, the process of calculation during

encryption/decryption can be reduced, and hence, encryption/decryption can be carried out easily at a high speed. Furthermore, since the cryptographic block number can be made small, a small-scale hardware is sufficient to construct a cryptographic communication system. As a result, the present invention can contribute to a development for the industrial realization of the product-sum type cryptography.

As this invention may be embodied in several forms without departing from the spirit of essential characteristics thereof, the present embodiment is therefore illustrative and not restrictive, since the scope of the invention is defined by the appended claims rather than by the description preceding them, and all changes that fall within metes and bounds of the claims, or equivalent of such metes and bounds thereof are therefore intended to me embraced by the claims.